Technical Evaluation Report

Workshop on Visualising Network Information IST-063/RWS-010

17-20 October 2006
The Royal Danish Defence College
Copenhagen, Denmark

Lisbeth M. Rasmussen
Chairman IST-063/RWS-010
Senior Research Advisor
Danish Defence Acquisition and Logistics Organization

lr@mil.dk

1. INTRODUCTION AND BACKGROUND

1.1 Introduction

The workshop brought together operational users, developers and researchers to explore the connection between visualisation technologies and network analysis for military and civil protection applications. NATO commanders, defence analysts, crisis managers etc., visualise the networks that affect their operations. Developers produce tools to assist network visualisation. Researchers discover the concepts and methods that developers turn into tools. In this context, networks include both "physical" networks, e.g. information and service infrastructure networks, as well as "conceptual" networks, e.g. social networks which show the interactions and organisational relationships among their elements. Application domains include: information assurance, infrastructure protection, network defence, network-enabled activities and counter-terrorism, along with peace keeping and peace support operations.

1.2 Background

The NATO R&T Organization Task Group, IST-059/RTG-025 ("Visualisation Technology for Network Analysis"), has been tasked with ascertaining the state of the art for network data presentation in various problem domains, determining the role and value of the underlying technology, and identifying promising technologies for visualising network information to support effective analysis (for more information, see http://www.vistg.net). In support of its mandate, the RTG initiated this latest in a series of bi-annual workshops addressing various aspects of information visualisation. In each of the previous two workshops — September 2002, "Massive Military Data Fusion and Visualisation: Users Talk with Developers" (IST-036/RWS-005), and September 2004, "Visualisation and the Common Operational Picture (COP)" (IST-043/RWS-006) — military officers and operators conducted problem-oriented discussions with visualisation researchers and system developers, in plenary sessions and in small focused working groups, to identify issues and recommend fruitful areas for research. Using the same methods, this workshop investigated how presentation technologies could be optimised for effective network visualisation.

1.3 Theme

The workshop had three integrated themes: Military and Civil Protection Applications, Human Factors, and Technology. The military application of visualisation technologies is overly simplistic and misleading, until the human factors related to comprehension and understanding are considered.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 DEC 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Technical Evaluation Report	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **The Royal Danish Defence College Copenhagen, Denmark**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM002067.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**4**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

2. PURPOSE AND SCOPE

The purpose of this workshop was to bring together those who use network analysis system, those who develop them, and those who make the systems more usable and effective. A core objective was to have users talk with developers and researchers. The workshop was supposed be a forum for commanders and staff officers to describe the pros and cons of current systems supporting network visualisation, which should help guide future military visualisation and research and development. The aim was to be multidisciplinary since both human factors and technological innovation collaborate in improving visualisation systems. The workshop intended to identify problems to which there are as yet no solutions, but where solutions seem possible.

3. EVALUATION

Overall, the combination of presentations (divided into three categories: "General/Theory", "Security & Defence" and "Medical"), plenary discussion and working groups provided comprehensive coverage of visualisation of network information and related human factors. Unfortunately there were not as many participants as expected, which was possibly due to:

- Poor dissemination of information among European institutions about the existence and nature of the workshop
- Academic institutions did not know of the possibility that they could ask for invitations
- Vacation time in Denmark.

In spite of this there was a stimulating interchange throughout the workshop and all working groups had participants from government/military, academia and industry.

The following points are particularly significant.

Social Network Analysis (SNA) is the mapping and measuring of relationships and flow between people, groups, organizations, computers, web sites, and other information/knowledge processing entities. The nodes in the network are the people and groups while the links show relationships or flow between the nodes. This makes SNA an important tool when fighting terrorism. SNA is multidisciplinary involving several aspects of both information science and human factors. The first keynote speaker Dr. Kathleen M. Carley from Carnegie Mellon University has taken SNA a step further to Dynamic Network Analysis (DNA) where the relationships are dynamic. It is still an emergent technology, but one to watch.

Network Centric Warfare, Network Enabled Operations, Network Enabled Capability, Network Centric Operations are the terms different nations use for the same concept, transforming to take advantage of the Information Age. It is about using networks to speed up and improve the C2 process. It is necessary to maintain the networks in support of operations, and to do that C2 must be extended to networks and cyberspace. An integrated information environment is required for this, and usually there are four environments:

- The unclassified Internet
- The designated Intranet
- The classified Command and control systems
- The special classified networks for areas such as Intelligence.

Today network visualisation shows a logical view of the networks with an indication that data is or is not flowing between routers (green meaning data is flowing and red meaning it is not). It is not an acceptable indication of availability. There might not be adequate bandwidth to pass the traffic. The network operators are happy as long as the indications are green, when in fact the user's needs might not be met.

There is no geographical representation of the network, so the network operations staffs have no idea as to whether an outage impacts an operation or not. How can they prioritize which problem to address first?

They are, in general, unaware that upgrades are being rolled out, which are often the cause of problems.

For all intents of purpose our Network staffs are blind, unable to make timely, prioritized decisions regards network repairs. This is certainly an unacceptable condition for Network Enabled Operations!

Network technology allows the commander to centralize command and control but this goes against the concept of decentralized elements that carry out operations. It is doctrine that will keep the joint chiefs out of the commander's backyard.

Visualising networks with thousands of nodes will overload the user, so it is necessary to reduce the complexity of the network. It is even difficult to visualise networks of more than 50 nodes. Several ways to attack this problem were discussed, but no solution yet.

The Medical session showed that co-operation on network visualisation between the medical science and information technology communities will benefit both in several areas:

1) There is similarity between computer viral transmission and biological viral transmissions. They both attempt to track and investigate the infection after the infection has begun. If the virus is spread via email then the parallels are strong, but if it is a specifically targeted attack (by proxy or otherwise) then the parallels may not be so strong. Other parallels include susceptibility or lack of susceptibility based on inoculation and/or temperament of the user. But there is a specific difference between computer and biological viruses in that some computer viruses are programmed to strike on specific days. There are parallels to bio-terrorism because computer viruses are human-induced and a global infection can be very quick. The comparison is reasonable because the computer model can take in parameters for susceptibility. However, proximity is not a factor for computer virus propagation, so an analogy to a neural network would fit more appropriately.
2) There are strong parallels between Information Assurance practices and the discovery and containment of sexually transmitted diseases and infections.
3) There could be value in a real time social network display during an outbreak so that you can take actions to contain it. Visualisations can help to identify nodes with different characteristics.

The participants were divided into 5 working groups. One group had a fixed topic "Framework" where a group of participants mainly from IST-059 worked on the framework that is part of their deliverables. The other four groups chose their topics. Three groups chose the topic "Reliability and uncertainty in situation awareness of Network Visualisation", and the last group worked on the topic "Vulnerability and Risk Assessment"

4. CONCLUSIONS

Most network information sets do not take "time" into account.

Network analysis and visualisation are:

1) Important tools in the fight against terrorism
2) Useful for tracking disease and attacks on computer systems (virus etc.)

Better view of the networks and what is occurring on them is needed. Multiple views of the network are needed:

- A logical view that shows communications links, routers, servers, firewalls and applications.
- A physical view that overlays the logical view on a geographical representation.
- A transactional view that shows if the various applications are functioning. Is logistics delivering just in time supplies? Are invoices being paid on time?
- An operational view that shows commanders and staff are able to use the networks to gain the advantage that Network Enabled Ops promises. Network staff can prioritize restoral on the basis of operational priorities.

There is not enough collaboration between the academic researchers and the defence community. The academic researchers would like realistic information to test their systems. If the systems are not tested on realistic information they might not be developed into useful systems for defence.

There is a critical need for advancing network Command and Control.

Progress has been marginal in the Network Operations Centres.

The two topics chosen by the workgroups "Reliability and uncertainty in situation awareness of Network Visualisation" and "Vulnerability and Risk Assessment" are important topics needing more research.

5. RECOMMENDATIONS

Contact between users, developers and researchers should be encouraged.

The problems need to be defined to be solved in ways that even civilian researchers may work on them. Better ways to get laundered data to researchers/modellers should be established.

Operational studies and analyses of visualisation needs from the analyst's and commander's viewpoints should be initiated.

A seamless environment across Net Ops Centres and R&D Labs should be created and R&D results should be used in the Ops Centres as soon as possible.

One "low hanging fruit" is to use higher resolution display technology or an appropriately matrixed array of high resolution displays oriented in such as manner as to maximize the information availability without "overloading" the user. Further research may improve how displays of this calibre can be organized to maximize the information output without creating an overload situation.

Experimentation with 3-D visualisation should be encouraged.

More research on "Reliability and uncertainty in situation awareness of Network Visualisation" and "Vulnerability and Risk Assessment" should be encouraged.

Concerning uncertainty and reliability the following is necessary:

- A clear definition of reliability and uncertainty is needed.
- Development of visualisation concepts and prototypes, defining what uncertainty and reliability conveys.
- Conduct experiments with representations of uncertainty and reliability.
- Development of consistent techniques for determining uncertainty and reliability.
- Development of intuitive techniques for visualising uncertainty and reliability.